



Infrastructure Security Challenges for the Defense Industrial Base

NDIA Homeland Security Symposium

Capt Bob Magee OUSD (IP)
June 17, 2003



Overview

- Critical Infrastructure Protection (CIP)
 - Defense Industrial Base Linkage
- Industrial Policy
- Defense Industrial Base (DIB)
 - Current Activities
 - Initiatives
 - Outreach/Awareness
 - Lessons Learned
- Discussion



What is Infrastructure Protection?



For the Department of Defense, Infrastructure Protection is Mission Assurance - the ability to mobilize, deploy and sustain U.S. military operations.

Interdependencies among critical infrastructure assets is key.





Why Infrastructure Protection?

- Lessons of History
- Changing Battlespace
 - Asymmetric Threat
 - Transformation of Industrial Base
- Failure of infrastructure assets that are critical will degrade or disrupt DoD operations
 - “Our challenge in the 21st century is to **defend our cities and our infrastructure from new forms of attack** while projecting force over long distances to fight new and perhaps distant adversaries.”
Secretary Rumsfeld Speaks on "21st Century Transformation" of U.S. Armed Forces

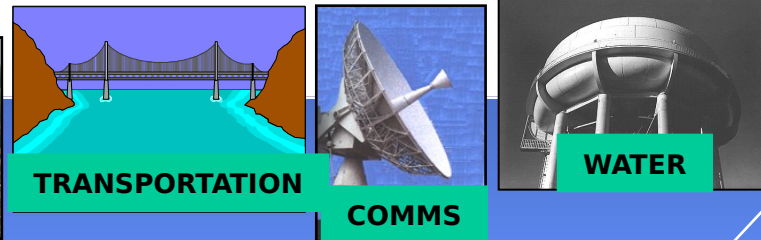


Critical Infrastructure (Linkages)

U.S. Military Depends on Commercial Support



INSTALLATIONS - PORTS - VITAL INDUSTRY



INFRASTRUCTURE



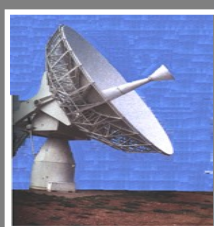


DoD Critical Infrastructure

Defense of the
Nation
&
Global Force
Projection

Defense Infrastructures

Personnel
Health
Financial
Services &
Transportation
C4I (Including the
Public
Work Surveillance & Recon
Defense Industrial Base



- Attempts to ensure DoD and non-DoD assets (sites & services) are available to **support military operations**
- Improves **dependability** of the vital assets
- Increases the options open to decision makers
- Limits **impact to the operation** if the assets are degraded or disrupted



Range of Interdependencies

President's Intent -- Pursue all necessary measures to eliminate significant vulnerabilities to both physical and cyber attack on critical infrastructures.

U.S. Federal Infrastructures U.S. Department of Defense Infrastructures

- | | | | |
|--------------------------------|---|-------------------------------------|---|
| • Information & Communications | ↔ | • Command, Control & Communications | • Intelligence, Surveillance & Reconnaissance |
| • Electrical Power | ↔ | • Public Works | • Personnel |
| • Gas & Oil | ↔ | • Public Works | • Space |
| • Banking & Finance | ↔ | • Financial Services | • Logistics |
| • Transportation | ↔ | • Transportation | • Health |
| • Water Supply | ↔ | • Public Works | • Defense Industrial Base |
| • Emergency Services | | | |
| • Government Services | | | |

DoD Scope:
- Domestic and Foreign
- Public and Private Sectors



Defense Industrial Base

Industrial Policy Focus:

- Ensure viable Defense Industry to support the Warfighter
- Health of the defense industry (USD AT&L goal)
 - Financial
 - Competition & Innovation
 - Support major defense system acquisitions
 - Anti-trust & Committee on Foreign Investment in US (CFIUS)
 - Product Sector Analysis
 - Critical supplier base
 - Niche or unique equipment
 - Security of supply/supplier base
 - Transformation
 - Battlespace Awareness, Command and Control
 - CIP for the Defense Industrial Base



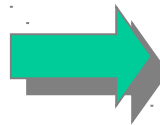
Defense Industrial Base Dynamic Landscape

Transformation of Industry

Inception Through Cold War

- Numerous major suppliers
- Platform Centric
- Wholesale Approach
- Linear Orientation
- Functional Requirements
- Management Of "Supplies"
- Mobilize Via Inventory
- Instantaneous Buys
- Stove Piped Systems
- "Build" Software

**"Plan, mobilize
industry,
stockpile, transport"**



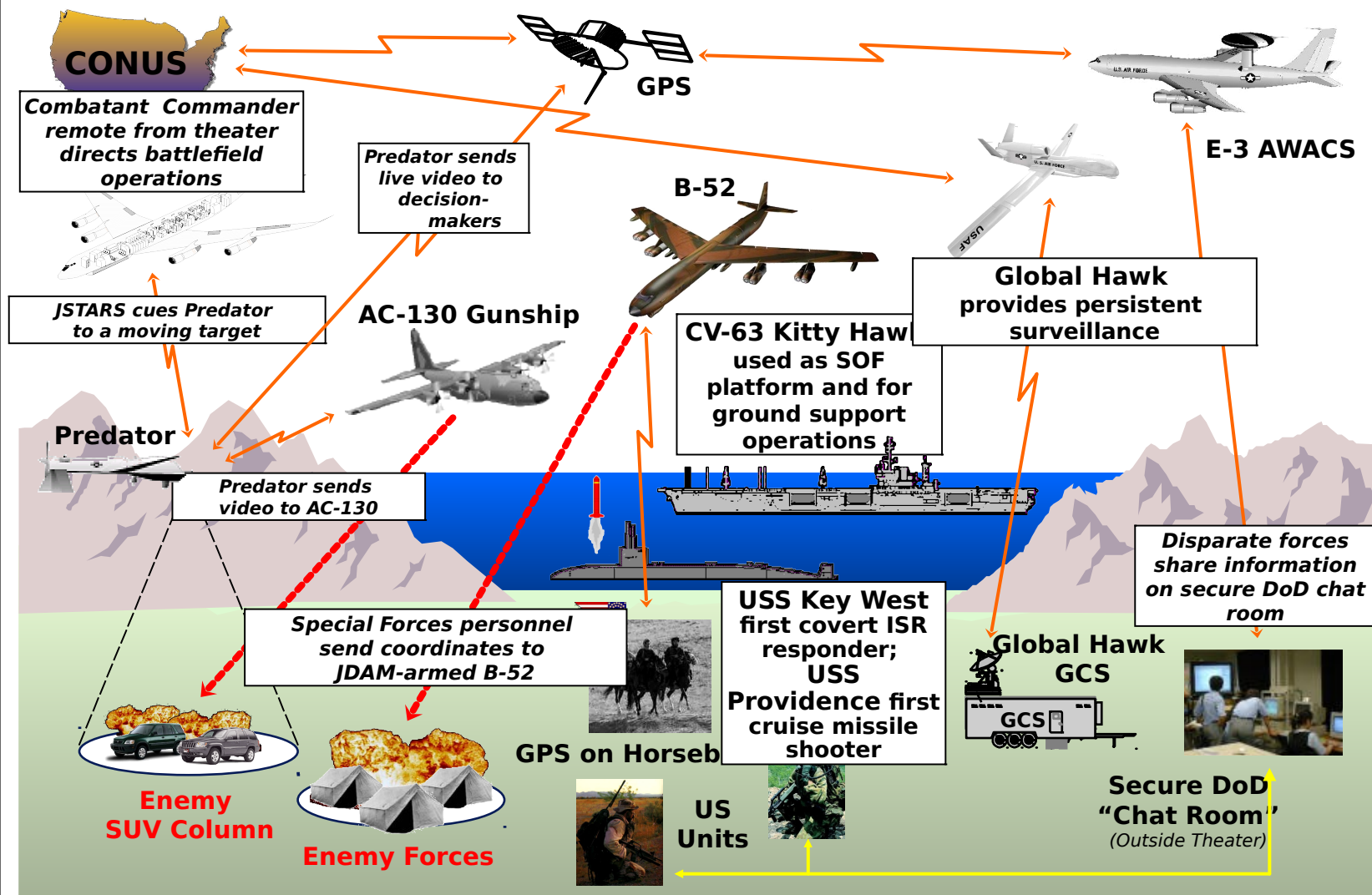
Today And Beyond

- Limited major suppliers
- Network Centric
- Retail Support to Customer
- Supply Chain Centric
- Outcome Oriented
- Management Of "Suppliers"
- Mobilize Via Industry
- Long Term Partnerships
- Open, Secure Architecture
- "Come as you are; just buy time delivery"
- "Buy/Assemble software"

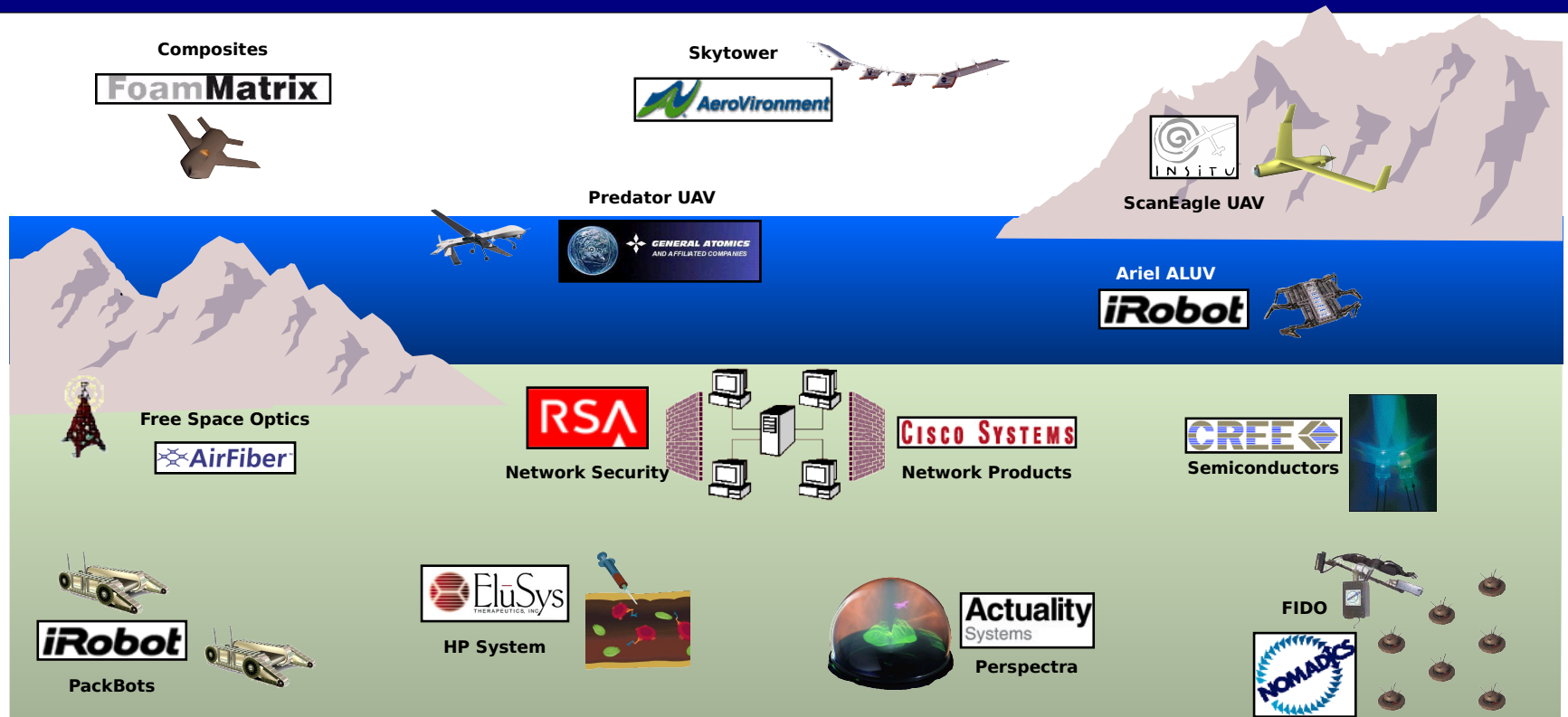
**"Come as you are; just
buy time delivery"**

"Buy/Assemble software"

TRANSFORMATIONAL CONCEPTS IN OEF & OIF



TRANSFORMATIONAL NETWORK-CENTRIC POSTURE OF EMERGING DEFENSE SUPPLIERS



SUPPLIER	TRANSFORMATIONAL PRODUCT
	PackBots: Man portable tracked ground vehicle
	Ariel ALUV: Autonomous Legged Underwater Vehicle
	ScanEagle: Low-cost, extremely long-range UAV
	Composites: UAV/UCAV Wings
	HP System: Anthrax vaccine
	Perspectra: Volumetric 3D Visualization Platform
	Predator UAV: Unmanned Aerial Vehicle

SUPPLIER	TRANSFORMATIONAL PRODUCT
	Network Security: Electronic encryption and protection
	Skytower: High altitude telecommunications UAV
	Free Space Optics: Last mile broadband wireless
	FIDO: Landmine and explosives detection
	Semiconductors: SiC and GaN products
	Network Products: Routers and switches



Defense Industrial Base CIP Challenges

- Coherent, Validated Methodology
 - Identification of Critical Assets
 - Identification of Interdependencies
 - Vulnerability Assessment Protocol
 - Risk Assessment Protocol
- Clarity of Threat, Actionable Indications and Warning
- Information Sharing & Protection
- Outreach and Education
 - Defense Industrial Base CIP Workshop-- NDIA/AIA 21 May 03

Sub-Tier Suppliers



Defense Industrial Base CIP Challenges (cont'd)

- DoD is lead for Defense Industrial Base (DIB)
 - Element of President's National Strategy
 - Information Coordination
 - NOT the deployment of troops to industry facilities
- Coordination with Critical Suppliers
- Threat and warning information sharing
- Support for vulnerability assessments
 - Three DIB sites funded
 - Supplemental
 - Self-assessment COTS software



Defense Industrial Base CIP Initiatives

- Updated Database of Critical Facilities
 - List provided to OASD C3I (CIP) and DSS. Database forwarded to Homeland Security and FBI.
- Connectivity and reporting enhanced
 - FBI outreach campaign
 - Joint Counter Intelligence Field Activity (CIFA) & Joint Counter Intelligence Assessment Group (JCAG) stood up by OASD C3I.
 - Linked with Joint Staff reporting system (TALON)
 - Local DSS and DCMA reps linkage for expediting reporting “suspicious activity” to chain of command and local law enforcement.
- CIP directive and instruction awaiting DepSecDef signature.
 - Increased emphasis on infrastructure security for defense contractors. Outlines general guidance for both classified and unclassified programs.



Defense Industrial Base CIP Awareness

- Outreach and Education Continuing
 - Industry Association Security reps regularly attend monthly CIP meetings.
 - Coordinating with OASD (C3I) and Industry Associations (NDIA, AIA) for Defense Industrial Base CIP workshops
 - DoD CIP Awareness CD-ROM containing CIP-related policies, documents, studies, and information briefings
 - FY 2002 DoD CIP Annual Report
 - COTS CD self assessment tool for CIP under review
 - Information Sharing Advisory Committee (ISAC) for Defense Industrial Base at National Level (DHS).
 - Stress Continuity of Business Operations and liaison with local law enforcement to corporate leadership
 - DSS/DCMA reps key
 - Reinforce through numerous industry forums.

Shareholder Equity



Lessons Learned

- Identification
 - Supporting direct military ops/sensitive work
 - Key sub-tier suppliers (Domestic and Foreign)
- Security
 - Beyond perimeter
 - Supporting Commercial infrastructure
- Continuity of Operations
 - Minimize impact
- Communication
 - Local, State, National agencies
 - Alert inform key suppliers
 - Ex. FBI field offices

<http://www.fbi.gov/contact/fo/info.htm>



Industry ISACs

Established ISACs

- Energy (Oil & Natural Gas) (www.energyisac.com)
- Financial Services (www.fsisac.com)
- Telecommunications
(www.ncs.gov/informationportal/portal.html)
- Electric Power (www.nerc.com/~filez/cipfiles.html/)
- Information Technology (<https://www.it-isac.org/>)
- Water Supply (www.amwa.net/isac/)
- Surface Transportation (www.surfacetransportationisac.org/)
- Emergency Fire Services (www.usfa.fema.gov/dhtml/fire-service/cipc.cfm)
- Food (www.fmi.org/)
- Chemicals Industry (<http://chemicalisac.chemtrec.com>)
- Emergency Law Enforcement
(www.nipc.gov/infosharing/infosharing5.htm)
- Interstate (www.nascio.org)



Information Sharing and Analysis Centers (ISAC)

- Value added features for members
 - Early Notification of Threats
 - Relevant Information
 - Industry-wide Vigilance
 - Subject Matter Expertise
 - Anonymous Information Sharing
 - Trending, Metrics, Benchmark Data
 - Secure database and analytic tools

Exposure



Summary

- Critical Infrastructure Protection (CIP)
 - Defense Industrial Base Linkage
- Defense Industrial Base (DIB)
 - Challenges
 - Initiatives / Outreach / Awareness
 - Lessons Learned



Questions

- Captain Bob Magee (703) 607-4045
– robert.magee@osd.mil